REPORT ON THE OVERARCHING PERSONAL INFORMATION PRIVACY FRAMEWORK FOR EXECUTIVE GOVERNMENT

June 15, 2004

Saskatchewan Information and Privacy Commissioner
100 – 1230 Blackfoot Drive
Regina, Saskatchewan
S4S 7G4
Website: www.oipc.sk.ca
Email: gdickson@oipc.sk.ca

Saskatchewan
Information and Privacy
Commissioner

100 - 1230 Blackfoot Drive
Regina, Saskatchewan
S4S 7G4

Tel: (306) 787-8350
Fax: (306) 798-1603
Website: www.oipc.sk.ca

June 15, 2004

Honourable P. Myron Kowalsky
Speaker of the Legislative Assembly
129 Legislative Building
Regina, Saskatchewan
S4S 0B3

Dear Mr. Speaker:

I am submitting to you and to the Members of the Legislative Assembly, in accordance with section 33(a) of the *Freedom of Information and Protection of Privacy Act,* my Report on the Overarching Personal Information Privacy Framework for Executive Government.

Respectfully submitted,

R. Gary Dickson, Q.C.
Saskatchewan Information and Privacy Commissioner

GD/ps
Encl.

104-06116/

TABLE OF CONTENTS

I Introduction 1-3

II The Freedom of Information and Protection of Privacy Act 5-8

III Overview of the Deloitte & Touche Privacy Assessment 9-10

IV The Deloitte & Touche Privacy Assessment 11-15

- Accountability 12
- Consent 12
- Recommendations 13
- Objectives 14-15

V Analysis of the Overarching Personal Information Privacy Framework for Executive Government 17-23

- Introduction 17
- Scope 18
- Vision 18
- Saskatchewan's Privacy Principles 19-22
  1. Accountability 19
  2. Purpose 19
  3. Limiting Consent 19-20
  4. Collection 20
  5. Use and Disclosure 20-21
  6. Retention 21
  7. Accuracy 21
  8. Safeguards 21
  9. Openness 21
  10. Access 22
  11. Compliance 22
- Goals, Objectives, Benchmarks and Actions 22
- Conclusion 23

TABLE OF CONTENTS

VI Summary of our Recommendations 25-28

VII Specific Areas of Concern and Recommendations 29-43

1. Training Government Employees 29
   (a) Who provides the training? 29-30
   (b) What is the Key Message? 30-33
2. Clarity is Essential 33-34
3. www.privacy.gov.sk.ca 34-35
4. Choices and Priorities 36
5. Proposal for a Chief Privacy Officer 37-38
6. Proposal for a Privacy Officer 39-40
7. Amending the FOIP Act 41-43

VIII Conclusion 45

I INTRODUCTION

On September 2, 2003 the Government of Saskatchewan released a document entitled *An Overarching Personal Information Privacy Framework for Executive Government.* [1] In that document ("the Framework") the Government asserts that "*This Privacy Framework is designed to place Saskatchewan at the strongest possible privacy protection policy position, while balancing the Government's need to meet its public policy obligations.*"

The document is described as follows:

> "*This Framework is the overarching corporate government mechanism for setting out its direction with respect to privacy matters. It is intended to ensure a balance between the privacy rights of individuals with respect to personal information and the legitimate needs of government departments and agencies in fulfilling their public interest mandate. At the same time, the purpose is to raise, for individual citizens, the level of protection of their personal information.*"
>
> *The intended audience of this document is Executive Government. The main intent is to state the privacy policy expectations of government and to provide this Framework for the implementation of those policy decisions. This is also a public document provided to inform citizens about what is being done to protect personal information.*
>
> *The objectives of this Framework are to:*
>
> - *Support the development and implementation of specific policies and procedures that recognize the particular circumstances of the departments and agencies.*
> - *Support the focused development and implementation of consistent personal information policies and procedures.*
> - *Provide benchmarks for the adoption and implementation of the personal information policies and procedures.*
> - *Provide processes for identifying and addressing inadequacies in the existing privacy policies, standards and practices, now and into the future.*

[1] Available at www.privacy.gov.sk.ca

I INTRODUCTION (CONTINUED)

> *In order to achieve these objectives, this Framework is comprised of a vision, principles, and goals that guide further policy development. Further, it provides objectives, benchmarks, and actions aimed at achieving the vision. It does not provide the policies that result from the identified actions. Rather it provides the vision, principles and context for these policies to be developed over the next few years. This Framework provides a common basis for policy development at the department or agency level.*
>
> *This document sets out the Privacy Framework as a permanent, yet continually developing statement of direction and action."*

The office of the Saskatchewan Information and Privacy Commissioner was not consulted in the development of the Privacy Framework. Since November 2003 this office has attempted to gather more information about the intention and plans of the province. We have also raised a number of questions and communicated concerns to the Executive Council and the Department of Justice. We want to acknowledge the candour and cooperation of both offices. The dialogue our office has had with both Justice and Executive Council has been very helpful in better understanding the intentions of government.

It is important to acknowledge some excellent work currently underway under the auspices of the Framework. We want to particularly signal our support for the work that has been undertaken by the Provincial Archives in the development of Records Retention and Disposition Schedules for government institutions. The Information Commissioner of Canada, the Honourable John Reid, has stated that "*information management is becoming more widely recognized as a core discipline of public sector management*".[2] The Provincial Archives work now in progress in Saskatchewan appears to be very consistent with the sharper focus on information management evident in other Canadian jurisdictions. We would suggest that one of the most substantial benefits to government institutions from the *Freedom of Information and Protection of Privacy Act* ("the FOIP Act") is the external discipline it imposes on those organizations to improve their record management capability.

We have been impressed with work currently underway in terms of addressing stronger security through information technology. This includes development of a comprehensive information technology security policy and guidelines for information protection classification for Saskatchewan government institutions. We have met with the Chief Information Officer and his officials to learn more about this work. We encourage government to continue these initiatives.

We have been advised by the Government that the Framework is very much a work in progress. We have been further advised that the specific elements of the Framework need a good deal more development and clarification. It is in the spirit of contributing to that process that we offer this analysis and our recommendations.

---

[2] 2002-2003 Annual Report , p. 32, available at http://www.infocom.gc.ca

I INTRODUCTION (CONTINUED)

Our office has no reason to believe that the Government's original assignment to Deloitte & Touche and the consequential Framework have been driven by anything other than a genuine interest in moving towards one of the highest public sector privacy standards in Canada. Our concerns with respect to the Privacy Framework can likely be attributed to unintended consequences of this Government initiative.

Given the ambitious scope and the far reaching implications of the September 2, 2003 document, we have determined that it is appropriate that we provide commentary on this initiative. The purpose is to provide information to Members of the Legislative Assembly and the people of Saskatchewan about the Framework and its impact on their information rights as guaranteed by the *Freedom of Information and Protection of Privacy Act* ("the FOIP Act") and the *Local Authority Freedom of Information and Protection of Privacy Act* ("the LA FOIP Act") and the *Health Information Protection Act* ("the HIPA").

The specific authority for our commentary is section 33(a) of the *FOIP Act* that provides as follows:

> "The [Saskatchewan Information and Privacy] Commissioner may: (a) offer comment on the implications for privacy protection of proposed legislative schemes or government programs…" [s. 33(a) FOIP Act]

The Privacy Framework is stated to be a direct response to a February 2003 report, the Government of Saskatchewan, Privacy Assessment.[3] This was prepared by Deloitte & Touche and reflected privacy assessments of 17 departments and Crown Corporations. The report identified a number of potential next steps and made 11 recommendations to Government as a whole. These eleven recommendations were in addition to the several recommendations made to each of the 17 departments and Crown Corporations.

The first recommendation was:

> "*1. **Overarching Privacy Framework** – The Government of Saskatchewan should develop an overarching privacy framework including supporting policies for all of the government departments and Crown Corporations that we examined. This Privacy Framework should recognize the need to balance privacy rights of the individual with respect to their personal information and the legitimate needs of the departments and the Crown Corporations in fulfilling their public interest mandate."* (p. 13)

The response by the Saskatchewan government to this recommendation is the Privacy Framework. This report will consider in more detail both the Privacy Assessment and the Privacy Framework.

[3] Available at www.privacy.gov.sk.ca

(THIS PAGE LEFT BLANK INTENTIONALLY)

II THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

This provincial law was proclaimed in 1992 and is similar to other access to information and privacy laws in every other Canadian province and territory. It is modeled to some extent on the federal *Access to Information Act* and the federal *Privacy Act* that went into force twenty-two years ago.

The Saskatchewan Court of Appeal has described the *FOIP Act* as follows:

> *The* [Freedom of Information and Protection of Privacy Act's] *basic purpose reflects a general philosophy of full disclosure unless information is exempted under clearly delineated statutory language. There are specific exemptions from disclosure set forth in the Act, but these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act. That is not to say that the statutory exemptions are of little or no significance. We recognize that they are intended to have a meaningful reach and application. The Act provides for specific exemptions to take care of potential abuses. There are legitimate privacy interests that could be harmed by release of certain types of information. Accordingly, specific exemptions have been delineated to achieve a workable balance between the competing interests. The Act's broad provisions for disclosure, coupled with specific exemptions, prescribe the "balance" struck between an individual's right to privacy and the basic policy of opening agency records and action to public scrutiny."* [4]

Our office has taken the position, in interpreting and applying the *FOIP Act* that the purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by:

- giving the public a right of access to records
- giving individuals a right of access to, and a right to request corrections of, personal information about themselves
- specifying limited exceptions to the rights of access
- preventing the unauthorized collection, use or disclosure of personal information by public bodies, and
- providing for an independent review of decisions made under the *FOIP Act* [5]

[4] General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance (Sask. C.A.) [1993] S.J. No.601
[5] Report #2004-003, available at www.oipc.sk.ca

II THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (CONTINUED)

Part IV of the *FOIP Act* sets out a complete 'code' for the collection, use, disclosure, access to and correction of personal information in the possession or control of a Saskatchewan government institution. A government institution includes all departments of government, Crown Corporations and a substantial list of boards, commissions and agencies. The number of "government institutions" exceeds 70.

Responsibility for each government institution is vested in the "head" of that institution. For government departments the head is the Minister. This vesting of responsibility in each Minister is significant. A provincial government is a large and complex entity. Making each Minister responsible for FOIP compliance within his or her Department ensures that there is a more meaningful kind of accountability.

The definition of what is personal information is contained in section 24. Collection is governed by sections 25 and 26. Government is enjoined by section 25 from collecting personal information "*...unless the information is collected for a purpose that relates to an existing or proposed program or activity of the government institution.*"

The manner of collection is codified in section 26. Where "reasonably practicable", personal information is to be collected directly from the subject individual unless one or more of 9 enumerated circumstances exists. One of the 9 exceptions to the direct collection requirement is where "the individual authorizes collection by other methods". There is no requirement for consent to collect personal information. If information must be collected directly from the subject individual, there is an obligation for the government institution to inform the individual of the purpose for the collection unless the regulations provide otherwise.

A government institution may use personal information with consent or without consent for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose; or for a purpose for which the information may be disclosed to the government institution without consent.[6] There are some 22 different circumstances which permit disclosure without consent. [7]

In summary, consent is not usually required for collection, use or disclosure provided the government institution is only collecting, using or disclosing for purposes directly related to its core purpose.

[6] Section 28
[7] Section 29

II THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (CONTINUED)

It is significant that we are aware of no Canadian jurisdiction that has elected to codify a consent-driven approach for its public sector privacy regime.

Section 31 prescribes a right of access by an individual to that person's personal information. Section 32 prescribes a right to request correction of an individual's record in the possession or control of a government institution.

In addition to the protection of privacy provisions in the FOIP Act, there is provision for access to general or non-personal records in the possession or under the control of a government institution. The access process is outlined in Part II. The mandatory and discretionary exemptions to disclosure are enumerated in Part III. Part V prescribes a process that a third party may follow to contest a proposed release of information that relates to that third party. The access provisions in the FOIP Act are linked to the privacy provisions in several ways:

- Any release of personal information in response to an access request from the subject individual under Part IV requires consideration of the Part III mandatory and discretionary exemptions.

- An individual requesting access to his or her personal information must follow the same process prescribed in Part II for an access request for general information.

- The review and appeal procedures in Part VII are common to both access for general information and access for personal information.

- For the greatest part, the powers and limitations of the Commissioner in Part VI and Part VII are common to both types of information.

The Supreme Court of Canada has carefully considered the linkages between access to information and personal privacy in its consideration of the federal *Privacy Act* and the *Access to Information Act* in the decision of Dagg v. Canada (Minister of Finance).[8]

It is an offence to knowingly collect, use or disclose personal information in contravention of the *FOIP Act* or regulations. The maximum fine is $1,000 or imprisonment for not more than three months. [9]

[8] [1997] 2 S.C.R. 403
[9] Section 68(1)

II THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT (CONTINUED)

Oversight of the *FOIP Act*, the *Local Authority FOIP Act* and the new *Health Information Protection Act* (HIPA) is assigned by statute to the Saskatchewan Information and Privacy Commissioner. The Commissioner is appointed by the Legislative Assembly for a five year term.

The Commissioner has the power to conduct a formal review if an applicant requests that the Commissioner review a decision to deny access to records or failure of a government institution to make a correction. The Commissioner may also:

> " *(a) offer comment on the implications for privacy protection of proposed legislative schemes or government programs;*
>
> *(b) after hearing the head, recommend that a government institution:*
> *(i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and*
> *(ii) destroy collections of personal information that is collected in contravention of this Act;*
>
> *(c) in appropriate circumstances, authorize the collection of personal information in a manner other than directly from the individual to whom it relates;*
>
> *(d) from time to time, carry out investigations with respect to personal information in the possession or under the control of government institutions to ensure compliance with this Part.* "[10]

There has been no significant amendment of the *FOIP Act* in the 11 years that have followed its proclamation.

Like other Canadian jurisdictions, the Commissioner, through reports and recommendations, applies and interprets the privacy rules in Part IV of the *FOIP Act*. Since the first full time Commissioner was appointed in Saskatchewan, an OIPC website has been created and now includes Reports issued by the Commissioner under the *FOIP Act* and the other two provincial laws.

The Commissioner also undertakes public education by: producing educational materials, providing information sessions, by producing an E-newsletter -- the *Saskatchewan FOIP FOLIO*, and by means of informational material posted to the website, www.oipc.sk.ca.

[10] Section 33

III OVERVIEW OF THE DELOITTE & TOUCHE PRIVACY ASSESSMENT

Given the derivative nature of the Privacy Framework it is appropriate to first consider the foundational instrument, the Deloitte & Touche Privacy Assessment.

The decision of the Government to undertake this high level review of information privacy policies, procedures, controls and systems is praiseworthy. It evidences a genuine interest in objectively assessing strengths and weaknesses and then pursuing remedial action.

The ambitious scope of the Privacy Assessment has meant an unprecedented charting of areas that require attention and remedial action.

At the same time however, there a number of limitations and gaps in the Privacy Assessment. These raise concerns with at least part of the analysis and impair the utility of the Framework that is founded on that Privacy Assessment. In other words, flawed assumptions in the Privacy Assessment lead to flawed elements in the Framework.

The Privacy Assessment is consistent with private sector strategies to meet the Canadian Standards Association Model Code for the Protection of Personal Information ("the CSA Model Code")[11]. The Model Code was designed initially for purposes of voluntary compliance by Canadian businesses with a standard that meets the requirements of the 1995 European Parliament Privacy Directive[12]. The CSA Model Code has now been incorporated into the federal *Personal Information Protection and Electronic Documents* Act ("PIPEDA") as Schedule 1 to that law.

The European Union Privacy Directive adapted the 1980 *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*[13] developed by the Organization for Economic Cooperation and Development (OECD) to a legislative format. The Directive effectively prohibits trade by EU member nations with any jurisdiction that does not have adequate privacy protection.

The CSA Model Code is general in nature and for the most part non-prescriptive. It was intended that the CSA Model Code could be utilized as a kind of template and that industrial groups in Canada could modify and particularize the template to address the particular needs of their industry. One of the most prominent and distinctive features is that the CSA Model Code is consent-driven. In other words, subject to limited exceptions, consent of the individual is required to collect, use or disclose personal information about that individual.

[11] CAN/CSA-Q830-96
[12] Directive 95/46/ED, OJ L281 (1995) 0031-0050
[13] Available at http://www.oecd.org/dsti/sti/it/secur/index.htm

III OVERVIEW OF THE DELOITTE & TOUCHE PRIVACY ASSESSMENT (CONTINUED)

The CSA Model Code was not designed for government. The public sector in Canada has operated under legislated privacy rules for the collection, use and disclosure of personal information for some twenty years. The initial model was the federal *Access to Information Act* and the federal *Privacy Act*. The public sector legislation modified the OECD Guidelines to reflect certain public sector realities.

When public sector access and privacy laws were being developed, it was determined that it was neither feasible nor appropriate to require consent for governments to collect, use or disclose personal information for the delivery of important government services, such as education, social services and healthcare. This likely reflects a couple of factors:

- Governments require vast amounts of personal information to deliver the public services that citizens and ratepayers expect
- A consent requirement would significantly impair the efficient and timely provision of services to citizens
- A consent requirement would significantly increase the cost of delivering public services
- Some of the things for which government requires personal information include the assessment and collection of taxes, user fees and charges and information necessary to the management of services. These are things citizens may be reluctant to provide consent to enable.
- In light of the numerous accountability mechanisms that existed in the public sector, abuse of personal information was probably seen as a smaller risk than in the less-regulated private sector (at least prior to January 1, 2004).

As a consequence, public sector privacy rules are not consent based. Instead of consent, there were provisions to ensure that collection, use and disclosure of personal information was limited to that which was deemed necessary for the operations of each government department. This public sector approach is clear in Saskatchewan's primary public sector privacy law - the *Freedom of Information and Protection of Privacy Act.*

Overall, the Privacy Assessment reflects a lack of understanding of the nature and operation of the *Freedom of Information and Protection of Privacy Act* in this province and equivalent legislation in other Canadian jurisdictions.

IV THE DELOITTE & TOUCHE PRIVACY ASSESSMENT

We have not seen copies of communications between Deloitte & Touche and the Government with respect to the terms of reference for the contracted Privacy Assessment. We determined that what matters is the Privacy Assessment, its analysis and its recommendations, regardless of the specific instructions provided by government. In any event, since the Saskatchewan Government has accepted the Privacy Assessment and all of its recommendations, the original terms of reference are likely moot.

We will consider the elements of the Privacy Assessment in the same order that they are discussed in the Deloitte & Touche document. All page numbers in this section refer to the appropriate page of the Privacy Assessment.

It is likely that the most useful part of the Privacy Assessment is the analysis of privacy practices in the 17 departments and Crown Corporations. This analysis is based on the responses to a questionnaire discussed in the Privacy Assessment and based upon the CSA Model Code.[14]

It is noted in the Privacy Assessment that "*No jurisdictions have so far incorporated the CSA into their public sector legislation but are, nonetheless, reviewing their privacy practices and finding ways to use the CSA and other 'like' codes in developing government policy surrounding the protection of private information*" [15]

This assertion is inconsistent with our office's understanding of Canadian public sector developments. Since all Canadian provinces and territories already have privacy laws "customized" for the public sector those jurisdictions have no need to use the CSA or other private sector codes.

Deloitte & Touche compared the privacy processes they discovered in the departments and Crown corporations to the CSA Guidelines. They found *"areas for improvement when compared to quickly evolving privacy practices and to the CSA guidelines"* [16]

The Privacy Assessment also states that, *"Beyond compliance with the FOI Act, there currently is not an overarching Privacy Framework currently in place in the government as a whole or at the departments and Crown Corporations that we reviewed."* [17] Saskatchewan's *FOIP Act* should serve, as similar legislation in all other Canadian jurisdictions does, as the overarching privacy framework for the public sector in this province.

[14] Assessment, page 8
[15] Assessment, page 8
[16] Assessment, page 9
[17] Assessment, page 10

IV THE DELOITTE & TOUCHE PRIVACY ASSESSMENT (CONTINUED)

We note that the Privacy Assessment describes the *Freedom of Information and Protection of Privacy Act* as the *FOI Act* throughout the document. Our office has encountered similar references to the FOIP Act in dealings with government institutions. The fact however that some government employees may have focused on access to information to the exclusion of privacy does not render Part IV of the FOIP Act inapplicable or without full force and effect. In any event, this would be a matter for education on the applicable legislation and not reason to create a new regulatory instrument such as the Privacy Framework.

1. Accountability

Although none of the departments and Crown Corporations has a designated Privacy Officer, the executive in charge or the FOI Access Officer is often informally filling this role". [18]

This assertion is confusing. The provincial *2000 Access Directory* makes clear reference to "Freedom of Information and Privacy Administrative Coordinators" for purposes of the FOIP Act. We are not sure of the source for the label - "FOI Access Officer" as it appears in the Privacy Assessment. We do not know why the Assessment fails to recommend that Administrative Coordinators in this province do what their counterparts do in every other Canadian jurisdiction and deal with both access and privacy matters. This failure later leads directly to the recommendation for a new position – a Privacy Officer for each government institution.

2. Consent

The assumption that consent is the desired standard for the collection, use and disclosure is inconsistent with Part IV of the FOIP Act although it does accurately reflect the CSA Model Code. It is unfortunate that there is no explanation or discussion about the differences between the treatment of consent in the FOIP Act and the CSA Model Code.

[18] Assessment, page 11

IV THE DELOITTE & TOUCHE PRIVACY ASSESSMENT (CONTINUED)

3. Recommendations

The recommendation to require departments and Crowns to "...implement formal re-enforcement sessions to ensure that all employees understand their responsibilities under the "FOI Act" is well taken. [19]

The recommendation about accountability ignores the fact that there already exists very clear accountability for each department and Crown Corporation.[20]

The recommendation addressing "implied consent" ignores the fact that the FOIP Act does not contemplate and does not sanction implied consent. [21]

The recommendation for data classification is very positive.[22]

The recommendation for limiting use, disclosure and retention ignores the requirements and guidance that already exists for use and disclosure in the FOIP Act.[23] There is a clear need for the development of operational procedures for retention and destruction of personal information consistent with the requirements of the FOIP Act.

The recommendation for safeguards is important since this is a serious omission in Part IV of the FOIP Act.[24]

The recommendations for contracts, implementing security initiatives and regular reviews are all important.[25]

There may well be value in considering the notion of an annual sign-off by employees but the more important consideration is providing each employee with the information they need to understand their legal requirements.[26]

---

[19] Recommendation 2, Assessment, page 13
[20] Recommendation 3, Assessment, page 13
[21] Recommendation 4, Assessment, page 13
[22] Recommendation 5, Assessment, page 13
[23] Recommendation 6, Assessment, page 13
[24] Recommendation 7, Assessment, page 14
[25] Recommendations 8, 9, 10, Assessment, page 14
[26] Recommendation 11, Assessment, page 14

IV THE DELOITTE & TOUCHE PRIVACY ASSESSMENT (CONTINUED)

4. Objectives

This section fails to acknowledge the differences between the CSA Model Code and the FOIP Act, particularly around the treatment of consent for collection, use and disclosure.

In the assumptions in the Limitations section[27] we note that the FOIP Act is described along with "other legislation governing privacy" as constituting a legislative framework. This legislative framework is then described as forming "... *one of the basis for the project*". Again, we do not understand the need to invoke the CSA standard and to do this without even acknowledging the differences between the CSA Model Code and the FOIP Act.

We note the comment that "*...the appropriate measure is to compare the practices of the Government departments and Crown Corporations against current practices in the Canadian public sector and by using the CSA Standards as a guide*"[28] In our view, the CSA Standards are not the most appropriate guide for this purpose and result in confusing messages to government staff and the public alike.

Later in the Privacy Assessment it is noted that "*The 10 principles of the Q830 standard require much more rigor than may currently exist in provincial public sector legislation that focuses on the protection aspects and therefore confidentiality, and not on the collection, use and disclosure aspects required when dealing with privacy.*" [29] We do not understand this assertion. Part IV of the FOIP Act is very much focused on the collection, use and disclosure of personal information. It could certainly be argued that Part IV is weak in terms of confidentiality since there is no express security/safeguarding obligation.

"*While adoption of the CSA Privacy principles in Private Sector privacy legislation will likely meet the "substantially similar" requirements of the Federal Personal Information Protection and Electronic Documents Act, our limited review did not identify any provinces that were currently addressing similar changes in their public sector Freedom of Information and Privacy legislation*" [30]. We agree with this observation but see this as yet another reason to question why the Privacy Assessment utilizes the CSA Model Code as its chief template.

---

[27] Assessment, Page 17
[28] Assessment, Page 18
[29] Assessment, page 20
[30] Assessment, page 23

IV THE DELOITTE & TOUCHE PRIVACY ASSESSMENT (CONTINUED)

There is a curious assertion that: *"As PIPEDA is based upon the CSA privacy principles, the adoption of the CSA Privacy Principles in Provincial private sector privacy legislation may result in a change in public sentiment, particularly if public sector privacy legislation is not similarly amended to provide individuals with the same privacy rights when dealing with government as will exist when dealing with the private sector."* [31] This is a questionable assumption that again seems to ignore the reality that the public sector already has customized privacy legislation carefully designed to not impede the important work of government.

Although we indicated earlier that we have not focused on the discussions as to the terms of reference for the Privacy Assessment, we note the following statement:
"The Government of Saskatchewan has asked us to use the CSA Privacy Principles to evaluate the current state of the protection of personal information within the 17 identified departments and Crown Corporations." [32]

We note that the tendency in parts of the Privacy Assessment to minimize or ignore the provisions of Part IV of the FOIP Act is apparent again in the section entitled Canadian Standards Association Privacy Principles[33]. The four page section on *Principle 7 – Safeguards* ignores perhaps the most serious gap in the terms of legislated privacy protection. This is the omission in the FOIP Act of any requirement on the part of a government institution to safeguard the personal information in its possession or control.

[31] Assessment, page 24
[32] Assessment, page 25
[33] Assessment, pages 25-53

(THIS PAGE LEFT BLANK INTENTIONALLY)

V ANALYSIS OF THE OVERARCHING PERSONAL INFORMATION PRIVACY FRAMEWORK FOR EXECUTIVE GOVERNMENT

We will consider the analysis and recommendations in the Privacy Framework using the same headings that appear in that document.

Introduction

This clearly identifies that this instrument has been designed to implement the Deloitte Touche Privacy Assessment. This is problematic for reasons outlined above in consideration of the Privacy Assessment.

This includes the recommendation #1 that

1. *Overarching Privacy Framework- The Government of Saskatchewan should develop an overarching privacy framework including supporting policies for all of the government departments and Crown Corporations that we examined. The Privacy Framework should recognize the need to balance privacy rights of the individual with respect to their personal information and the legitimate needs of the departments and the Crown Corporations in fulfilling their legitimate public interest mandate."*[34]

This recommendation begs the question - since Saskatchewan already has comprehensive access and privacy legislation that covers all government departments and Crown Corporations, what value does this Privacy Framework add, if any? Although we take issue with some of the analysis in the Privacy Assessment, we acknowledge much useful work and information in the assessment of strengths and weaknesses in each of the 17 departments and Crown Corporations. The Privacy Framework document, on the other hand, does not in our view add significant value to the legislation currently in force. Its chief value may be in signaling to the people of Saskatchewan the seriousness with which the government takes its responsibility to respect their privacy. In the early stages of the Framework it has engendered considerable confusion.

Although the *FOIP Act* constitutes a comprehensive set of rules for personal information, it has deficiencies and will require amendment to achieve the purposes that Saskatchewan courts and our office have ascribed to it. The Office of the Information and Privacy Commissioner takes the position that statutory amendment is a much better way of addressing deficiencies than the creation of new and different rules by means of a policy statement.

[34] Framework, page 13

V ANALYSIS OF THE OVERARCHING PERSONAL INFORMATION PRIVACY FRAMEWORK FOR EXECUTIVE GOVERNMENT (CONTINUED)

Scope

"*This Framework has been designed to build on the current legislation, but in case of conflict of interpretation the Acts shall prevail*".[35] We think this claim is problematic since the Framework is based on a very different set of values than Part IV of the *FOIP Act*. There are areas where they correspond, but enough differences to make this claim confusing.

Vision

The vision[36] could equally describe Part IV of the *FOIP Act*. It would be useful to do what many other jurisdictions have done and include a statement of purpose in Saskatchewan's *FOIP Act*. The incorporation of such a vision in a piece of legislation is much stronger and more meaningful than a policy declaration. The British Columbia provision is as follows:

"The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by:

(a) giving the public a right of access to records,

(b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,

(c) specifying limited exceptions to the rights of access,

(d) preventing the unauthorized collection, use or disclosure of personal information by public bodies, and

(e) providing for an independent review of decisions made under this Act."[37] [emphasis added]

[35] Framework, page 7
[36] Framework, page 12
[37] Section 2(1) British Columbia *Freedom of Information and Protection of Privacy Act*

V ANALYSIS OF THE OVERARCHING PERSONAL INFORMATION PRIVACY FRAMEWORK FOR EXECUTIVE GOVERNMENT (CONTINUED)

Saskatchewan's Privacy Principles

This section is illogical and confusing. The main reason for the inappropriateness of the CSA Model Code is that it incorporates a consent based regime in a way that may impede the valuable and essential work of executive government. The Model Code is consent driven. Part IV of *FOIP Act* is not. This difference is not even referenced in this section of the Privacy Framework[38].

Why is the CSA Model Code *"a valuable reference point for the Saskatchewan Privacy Principles"*?[39] We believe that it would be much simpler and much more appropriate to focus on making Part IV of the *FOIP Act* the reference point.

1. Accountability

We can't see what value this section adds to the very clear assignment of responsibility in Part IV of the *FOIP Act* to the "head" of a government institution. We view it as confusing to suggest that someone other than the head may have responsibility.

2. Purpose

We do not see any value added to the very clear limitation on collection in section 25 of the *FOIP Act*.

3. Limiting Consent

This section of the Framework does not accurately reflect Part IV of the *FOIP Act*. The *FOIP Act* addresses when consent is required. The Privacy Framework states: "*Obtaining consent from the individual is the expected approach for the collection, use and disclosure of personal information, but it is not always feasible, appropriate, or the only legal means of authority.*"[40]

It goes on to say consent should be informed consent. This is different than the statutory requirement. "Informed consent" incorporates a whole set of challenges such as how the province deals with citizens with learning disabilities, language, cultural challenges and literacy issues. If a decision is made to import this significantly higher standard, this should be reflected clearly in the legislation not done by way of a policy statement.

[38] Framework, page 12
[39] Framework, page 13
[40] Framework, page 14

V ANALYSIS OF THE OVERARCHING PERSONAL INFORMATION PRIVACY FRAMEWORK FOR EXECUTIVE GOVERNMENT (CONTINUED)

3. Limiting Consent (continued)

The legal requirement for consent is clearly limited in sections 28 (for use) and section 29 (for disclosure).

Consent under FOIP must be *"in writing unless, in the opinion of the head, it is not reasonably practicable to obtain the written consent of the individual"*[41]
The Privacy Framework sanctions implied consent that is not clearly sanctioned in the *FOIP Act*.

The statement "*It is important for government to strive to obtain informed written consent where such is reasonably practical.*" [42] is likely to be confusing to government workers who must use a different test in the legislation.

Consent, when it is required and what form it will take is one of the problematic areas of privacy legislation. This section is not helpful and in fact is inconsistent with FOIP requirements.

4. Collection

This is already addressed in a comprehensive fashion in section 26 of the *FOIP Act*. We don't see this adding any value.

5. Use and Disclosure

Section 28 sets out very clearly the rules for use of personal information. That provides that "*No government institution shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except: (a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or (b) for a purpose for which the information may be disclosed to the government institution pursuant to subsection 29(2).*
Section 29(2) enumerates 22 different kinds of disclosures that do not require consent.

[41] *Freedom of Information and Protection of Privacy Regulation*, c. F-22.01 Reg 1 as amended, s. 18
[42] Framework, page 15

V ANALYSIS OF THE OVERARCHING PERSONAL INFORMATION PRIVACY FRAMEWORK FOR EXECUTIVE GOVERNMENT (CONTINUED)

5. Use and Disclosure (continued)

The statement in the Privacy Framework that "*Personal information shall be used or disclosed only for the purposes for which it was collected or for a use consistent with that purpose, except with the consent of the individual or as specifically authorized by law*"[43] is confusing since it does not draw attention to the broad opportunities for use and disclosure without consent. It is not at all helpful to orienting government workers to the use and disclosure rules under which they are statutorily bound to operate.

6. Retention

Retention is not addressed in the *FOIP Act* but ought to be.

7. Accuracy

The text in this document is different than section 27 of the *FOIP Act*.[44]

8. Safeguards

This is not addressed in the *FOIP Act* but ought to be.[45]

9. Openness

Transparency as to the procedures of any particular privacy regime is an important feature. The objective is to make information about the way a particular organization collects, uses and discloses personal information readily accessible. A citizen or government employee however will be challenged to find out precisely what is required in post-Privacy Framework Saskatchewan. That citizen will be required to resort to the *FOIP Act* (37 pages), the FOIP Regulation (16 pages) and now the Framework (51 pages) to understand what rules govern. This becomes more complicated since the Framework uses different rules and tests than the specific statute designed to address the information rights of Saskatchewan residents.

[43] Framework, page 16
[44] Framework, page 17
[45] Framework, page 18

V ANALYSIS OF THE OVERARCHING PERSONAL INFORMATION PRIVACY FRAMEWORK FOR EXECUTIVE GOVERNMENT (CONTINUED)

10. Access

The right to access one's own information is already clearly described in the *FOIP Act*. This statement provides no additional value.[46]

11. Compliance

This is confusing since the responsibility in the *FOIP Act* is clear.[47] It is the responsibility of the head. He or she may delegate to someone in their organization. If a Saskatchewan resident cannot get satisfaction dealing with the FOIP Coordinator, they have the right to appeal to the independent office of the Information and Privacy Commissioner.

Goals, Objectives, Benchmarks and Actions

"The Privacy Principles, in conjunction with the Commentary and the Legislative References, provide a foundation for action in government with respect to personal information."[48]

Our response is that the *FOIP Act* already functions as the appropriate foundation for action in government with respect to personal information. It does this through an elegant balance of the public's right to know and access government records and the need to protect privacy. The Privacy Principles accurately reflect private sector experience and needs but ignore the different challenges posed in regulation of the public sector. The Privacy Principles largely ignore extensive public sector experience in virtually every other Canadian jurisdiction.

"This Framework is intended to put an overall policy perspective on these activities, in order to achieve greater clarity, effectiveness, and efficiency."[49]

The existing *FOIP Act* provides a clear overall legislative perspective. Far from providing greater clarity, effectiveness, and efficiency, the Framework results in confusion and cumbersome new requirements apart from the existing legislative obligations.

---

[46] Framework, page 19
[47] Framework, page 19
[48] Framework, page 21
[49] Framework, page 21

V ANALYSIS OF THE OVERARCHING PERSONAL INFORMATION PRIVACY FRAMEWORK FOR EXECUTIVE GOVERNMENT (CONTINUED)

Conclusion

"*This Framework is intended to create the policy opportunity to move this important initiative forward and the accountability framework to hold government accountable to ensure that the actions are carried out at the appropriate levels.*" [50][emphasis added]

There already exists an accountability framework. This consists of legislated requirements, clear assignment of responsibility to the Minister of a Department and recourse to an independent officer of the Legislative Assembly. This framework exists and works effectively in every other province and territory in Canada and has for almost 20 years.

[50] Framework, page 28

(THIS PAGE LEFT BLANK INTENTIONALLY)

VI SUMMARY OF RECOMMENDATIONS

What follows is a summary of 15 different recommendations from the Office of the Information and Privacy Commissioner that build on our analysis of the Privacy Assessment and the Privacy Framework:

Recommendation No. 1 (See Page 29)

The training contemplated by the Framework should be undertaken by the department tasked with responsibility to administer the *Freedom of Information and Protection of Privacy Act* and not the Public Service Commission. This would mean that the Minister responsible for administration of the *FOIP Act* and responsible for preparation of the Annual Report prescribed by section 63 of the *FOIP Act*, would specifically be given responsibility for training all government employees to a good working knowledge of the Act and how it impacts their day to day activities. This Minister should also conduct or organize internal audits and assessments and recommend improvements and work with departments, agencies and the Archives to facilitate the implementation of records management systems that support privacy.

Recommendation No. 2 (See Page 30)

The privacy training of government employees should proceed only as an integrated element of training to both access and privacy requirements under the *Freedom of Information and Protection of Privacy Act*.

Recommendation No. 3 (See Page 32)

Training should focus, not on the CSA Model Code, but rather on the precise text of the *Freedom of Information and Protection of Privacy Act*. The sooner government employees become familiar with the provisions of the *FOIP Act*, the better. There is no added value in having employees cross-reference the *FOIP Act* with the CSA Model Code. We think it is likely this cross-referencing will prove a cumbersome and discouraging nuisance.

Recommendation No. 4 (See Page 33)

We encourage the Department that is assigned responsibility for training to carefully consider adaptation of excellent materials that have been developed in provinces such as Ontario, British Columbia and Alberta for this purpose.

VI SUMMARY OF RECOMMENDATIONS (CONTINUED)

Recommendation No. 5 (See Page 33)

There should be specific attention to ensure that those government employees who routinely deal with the public and those involved in records management are provided with training that allows them a comfortable understanding of what they can and cannot do with the personal information of Saskatchewan residents.

Recommendation No. 6 (See Page 34)

The website, www.privacy.gov.sk.ca, should be modified to address compliance with all parts of the *Freedom of Information and Protection of Privacy Act* and not just the Framework.

Recommendation No. 7 (See Page 36)

All government institutions should ensure that compliance with section 16 of the *Health Information Protection Act* is given the priority the law requires and must take precedence over any Privacy Framework activities.

Recommendation No. 8 (See Page 38)

The Chief Information Officer should be given specific responsibility for incorporating privacy protection in all information systems of the Government and for ensuring that legislative requirements are met.

Recommendation No. 9 (See Page 39)

For every Government institution, there should be one person designated as the Freedom of Information and Privacy Coordinator with responsibility for the FOIP Act including both access and privacy requirements. This FOIP Coordinator should be a senior manager in the government institution and should report to the Deputy Minister

VI SUMMARY OF RECOMMENDATIONS (CONTINUED)

Recommendation No. 10 (See Page 39)

Recommendation No. 10 -- The FOIP Coordinator should be required to do the following:

- respond professionally and efficiently to access requests and privacy complaints, and;
- raise awareness of access and privacy issues on a regular and proactive basis within their organization;
- be well aware of all operations of the organization, the kinds of records and record-management systems in the department;
- be able to quickly identify what units within the department are likely to have the records responsive to an access request and which employees should be consulted;
- be senior enough to be able to provide access and privacy advice to the Deputy Minister or head of the organization on a regular basis;
- monitor decisions and recommendations of the OIPC and ensure those decisions are integrated into the orientation and in-service training of staff in the Department;
- be involved in the design of new programs that may impact access or privacy rights;
- provide timely advice to the Department to ensure that the *FOIP Act* will be complied with; and
- improve general awareness about the legislation and also substantive items such a specific recommendations from the OIPC. This can be done through regular in-service training sessions within a department. The Coordinator may undertake internal audits to identify areas where more work is required to ensure full compliance.

Recommendation No. 11 (See Page 41)

The *Freedom of Information and Protection of Privacy Act* should be reviewed by an all-party committee of the Assembly to determine what changes to the statute and government policies and practices are necessary to ensure an adequate level of access and privacy in Saskatchewan.

VI SUMMARY OF RECOMMENDATIONS (CONTINUED)

Recommendation No. 12 (See page 41)

Recommendation No. 12 – The *Freedom of Information and Protection of Privacy Act* should include an explicit purpose clause. We propose the following text:

> The purposes of this Act are to make government institutions more accountable to the public and to protect personal privacy by:
>
> (a) giving the public a right of access to records,
>
> (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,
>
> (c) specifying limited exceptions to the rights of access,
>
> (d) preventing the unauthorized collection, use or disclosure of personal information by government institutions, and
>
> (e) providing for an independent review of decisions made under this Act.

Recommendation No. 13 (See Page 42)

The *Freedom of Information and Protection of Privacy Act* should be amended to include a requirement that the head of a government institution must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and destruction.

Recommendation No. 14 (See Page 43)

The *Freedom of Information and Protection of Privacy Act* should be amended to permit the use and disclosure of personal information, subject to appropriate safeguards, to enable 'shared services' such as the SCHOOLPLUS initiative.

Recommendation No. 15 (See Page 43)

The *Freedom of Information and Protection of Privacy Act* should be amended to signal the seriousness of privacy breaches by increasing the penalties to something more substantial such as a maximum fine of $50,000 for an individual and $100,000 for a corporation.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS

What follows is a more detailed consideration of certain particularly problematic features of the Framework and a number of recommendations.

1. Training Government Employees

We understand that there was a major effort by the Government to train government employees with respect to the *FOIP Act* at or about the time it first came into force in 1992. We are not aware of any government wide training initiative since that time and prior to the Privacy Framework. In the experience of our office, there are a relatively modest number of Saskatchewan government employees who have an in depth understanding of the *FOIP Act* and the way it operates. It is usually by means of working with a significant number of requests and complaints that government employees develop expertise and strengthen their skills. This experience is limited to some extent since historically there have not been large numbers of requests or complaints under the Act. We expect this in turn is attributable to the fact there has not been much done in Saskatchewan in terms of public information and promoting awareness of this important law. It may also be attributable in part to the lack of resources for past Information and Privacy Commissioners to address section 45(b) of the FOIP Act. That provision mandates the Commissioner "*to conduct public education programs and provide information concerning this Act and the commissioner's role and activities.*" Hopefully that will be ameliorated now that there are additional resources for the office of the Commissioner and the appointment is a full-time appointment.

We note the comment in the Deloitte & Touche Privacy Assessment that "*The* [FOIP] *Act was well known at all agencies we reviewed and processes have been in place for many years*" [51]. In the experience of this office, the Act is generally not well known, beyond a small number of individuals in each department. The total number of access requests and privacy complaints under the *FOIP Act* has been modest. A number of government departments have processed very few requests or complaints. We have not encountered any department that has developed a form of Privacy Impact Assessment, or that has in recent years provided its staff with FOIP training at a practical and work-relevant level.

There are two areas we wish to highlight in the training sphere:

(a) Who provides the training for employees?

The Framework tasks the Public Service Commission with responsibility for training. That Commission certainly has expertise in providing support to institutions in respect of the rules and policies for employees but we question whether it is the most appropriate agency to undertake privacy training.

[51] Assessment, page 22

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

(a) Who provides the training for employees? (continued)

In the experience of this office, training in privacy is best done by the department charged with administration of the statute. In Saskatchewan, the Department of Justice is responsible for the administration of the *FOIP Act*. Justice provides advice and support to all provincial departments on access requests and breach of privacy complaints as well as general information about the Act.

We note that the well established practice in other jurisdictions with a robust access to information and privacy regime is to vest training responsibility in the department responsible for administration of the access and privacy law. This appears to work very well in jurisdictions such as Ontario, British Columbia and Alberta. This means that those providing instruction have the practical experience of working with the law. They appreciate the nuances and practical issues that are so important to ensuring a first rate educational experience for government employees. Instruction in the statutory provisions is important but insufficient. It is just as important for government employees to understand how those provisions are applied and interpreted by the Saskatchewan Information and Privacy Commissioner, superior courts in Saskatchewan and in some cases, by oversight bodies in other jurisdictions.

Recommendation No. 1 – The training contemplated by the Framework should be undertaken by the department tasked with responsibility to administer the *Freedom of Information and Protection of Privacy Act* and not the Public Service Commission. This would mean that the Minister responsible for administration of the *FOIP Act* and responsible for preparation of the Annual Report prescribed by section 63 of the *FOIP Act*, would specifically be given responsibility for training all government employees to a good working knowledge of the Act and how it impacts their day to day activities. This Minister should also conduct or organize internal audits and assessments and recommend improvements and work with departments, agencies and the Archives to facilitate the implementation of records management systems that support privacy.

(b) What is the Key Message?

It appears that the key message in the Privacy Framework for the proposed training is protection of privacy. This is very important and certainly one of the key themes of the *FOIP Act*. As noted above however, there are two equally important themes in the FOIP Act: (1) **public information is accessible and (2) personal information is protected**. The training described in the Framework and plans announced to date by government focus exclusively on privacy.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

(b) What is the Key Message? (continued)

It is not good enough to train staff on the protection of privacy. That tends, in our office's experience, to put the focus on secrecy - on refusing to share information. We can find many examples in the early days of new privacy laws in Canada where employees, uncertain of what they can and cannot do and unwilling to make a mistake; simply tend to not disclose information even when disclosure is appropriate and authorized by law. A single-minded focus on privacy is likely to lead to a decided reluctance, at least in the near term, to disclose information. This is the antithesis of meaningful access to information- a process necessary to ensure government is kept accountable.

The Information Commissioner of Canada addressed this issue in his presentation to the symposium held at the University of Regina in May 2003 on *E-Government Reconsidered: Renewal of Governance for the Knowledge Age.*[52] The Commissioner observed as follows:

> "I have, up until now, been discussing the transparency part of the access-privacy duality. Let me now turn to the opacity part-that is, privacy. As Canada's Information Commissioner, I am required to investigate citizen complaints about government secrecy. I see close up, then, the ways in which the values of openness and privacy rub against each other.
>
> First, we must keep in mind that the right to privacy and the right of access to information are not inherently contradictory. The right to know is deeply imbedded in the right to privacy. A cornerstone-perhaps the very foundation- of the right to privacy is the right of individuals to know what information governments and, now, private firms, hold concerning them. The two rights do not come into conflict until someone desires to know something personal about someone else. Some such desires are justifiable, some are not.

[52] Edited by E. Lynn Oliver and Larry Sanders, Canadian Plains Research Centre and the Saskatchewan Institute of Public Policy, Regina, 2004

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

(b) What is the Key Message? (continued)

My experience is that it not very difficult to know when a privacy invasion is justified and when it is not. Yes, there are hard cases, but they are rarer than I expected. The key, it seems to me, is to bear in mind that both rights are designed to shift the balance of power from the state to the individual. Whenever access and privacy rights appear to be in conflict, an understanding of what I call the "accountability payoffs" almost always leads to a sensible resolution of the apparent conflict. For example, the privacy interests of public officials must, in a free and democratic society, be given less weight (in the balance with openness) than the privacy interests of private citizens.

The reason is obvious. It would be Kafkaesque to allow public officials to be nameless and faceless, closed-mouthed about their duties and functions or secretive about their perks and remuneration. There is a higher hurdle for public officials to clear in order to justify protecting their privacy over the public's right to know. I hasten to add that public officials should not be stripped of all privacy rights. The guiding principal is this: would invasion of a public official's privacy serve to improve the accountability of government or would it simply pander to public curiosity?"[53]

Recommendation No. 2 -- The privacy training of Government employees should proceed only as an integrated element of training to both access and privacy requirements under the *Freedom of Information and Protection of Privacy Act.*

We think it is important to ensure that government employees become familiar with the text of the *FOIP Act* and understand the key sections of that Act. Our recommendation is to replace reference to the 11 principles in the Privacy Framework with an outline of the primary duties under the *FOIP Act*.

[53] ibid, page 86

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

Recommendation No. 3 – Training should focus, not on the CSA Model Code, but rather on the precise text of the *Freedom of Information and Protection of Privacy Act*. The sooner government employees become familiar with the provisions of the *FOIP Act*, the better. There is no added value in having employees cross-reference the *FOIP Act* with the CSA Model Code. We think it is likely this cross-referencing will prove a cumbersome and discouraging nuisance.

Other provinces have developed extensive first-rate training materials that could easily be adapted to the Saskatchewan environment. Of particular value would be materials that have been prepared by the Ontario Management Board Secretariat, the Information Management Access and Privacy Division of Alberta Government Services and the Corporate Privacy and Information Access Branch of the British Columbia Ministry of Management Services.

Recommendation No. 4 -- We encourage the Department that is assigned responsibility for training to carefully consider adaptation of excellent materials that have been developed in provinces such as Ontario, British Columbia and Alberta for this purpose.

2. Clarity is Essential

Training staff in good information management presents a couple of obvious challenges. Since the creation, maintenance, storage and ultimate destruction of records is so fundamental to the operation of government institutions, it is important that the key messages be simplified and reinforced. If government employees are uncertain of what they can and cannot do, the risk is some degree of paralysis since staff may procrastinate taking any action with the record they are dealing with. This kind of paralysis obviously must be avoided to ensure that the important services of the Saskatchewan Government can be delivered in an efficient and cost-effective manner.

As noted above, the *FOIP Act*, and particularly Part IV, sets out a complete code for the collection, use, disclosure, access to and correction of personal information. In the experience of this office, the *FOIP Act* can be a challenging and tricky instrument for staff to master. It requires a lot of careful planning to develop those key messages and ensure they are consistent with the mandate conferred on government institutions by the *FOIP Act*.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

2. Clarity is Essential (continued)

It is not helpful to attempt to overlay the Framework, in its current form, over the *FOIP Act*. The only value added by the Framework we can see is a heightened awareness of privacy responsibilities of government departments. This heightened awareness comes at a substantial price – the confusion over conflicting messages. For reasons noted earlier, the Framework is essentially focused on a consent-driven regulatory scheme that is significantly different than the Act. This introduction of the CSA Model Code engenders confusion. Our office has witnessed this confusion in a number of government institutions currently wrestling with how to adapt the Framework to their particular information management requirements. Initially, we encountered this confusion in government departments but now have observed it also in some local authorities that have concluded that the Framework binds them.

In the experience of this office, the training must be for all government employees but in particular should target employees who routinely interact with the public in the course of their employment and also employees who are engaged in records management work including opening files, maintaining files and archiving and destroying files. This is one of the areas where the risks to confidentiality and security are greatest. To ensure full compliance, staff must have a comfortable understanding of what they can and cannot do with the personal information of Saskatchewan residents.

Recommendation No. 5 – There should be specific attention to ensure that those government employees who routinely deal with the public and those involved in records management are provided with training that allows them a comfortable understanding of what they can and cannot do with the personal information of Saskatchewan residents.

3. WWW.Privacy.gov.sk.ca

The Saskatchewan Government has recently created a website to promote privacy compliance - www.privacy.gov.sk.ca. Our assumption is that the website is targeted to government employees and perhaps employees of Saskatchewan Crown Corporations.

The creation of a website is an excellent means of providing uniform messaging to the entire government workforce but we have concerns with the content. For reasons identified earlier we are troubled with the attempt to segregate privacy and access and treat them as discrete matters. The website should be refocused on compliance with all elements of the *FOIP Act*, not just a portion of that statute.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

3. WWW.Privacy.gov.sk.ca (continued)

The website, in its original iteration, included a hyperlink to the Privacy Commissioner of Canada, although neither of the two statutes that Commissioner oversees, the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*, have any application to any provincial government department or provincial Crown Corporation. We understand that hyperlink has now been deleted. We support this action and encourage the Public Service Commission to do everything possible to focus employees of departments and Crown Corporations on compliance with the *FOIP Act*. This includes both access to information and privacy requirements.

One of the difficulties is how to ensure government employees understand not only the provisions of the Act but also another 56 pages of fairly ambiguous language in the Framework, and to then sort out how these two instruments are supposed to work together. The website information is for the most part too high level to provide much meaningful, practical advice to government employees.

We think it is unrealistic and an unnecessary burden to delegate to each department responsibility for taking the very general material currently available on the website and adapting that to a practical, detailed set of privacy rules. To ensure appropriate educational materials for a high standard of privacy protection, we think it will be necessary for a great deal more work to be done on a pan-government basis. We recommend that the site include the following:

1) An Introduction to FOIP module. This should embrace both access and privacy rules as well as the mechanics of a formal review or breach of privacy complaint and the role of the Office of the Information and Privacy Commissioner

2) A FOIP for Senior Officials module. This should focus on the practical things that senior managers need to understand to ensure full compliance within the department with the *FOIP Act*.

Case studies are an effective means of making the learning modules relevant and useful to government employees. Checklists are also useful for anyone who will be involved in responding to inquiries, complaints or review requests.

Recommendation No. 6 -- The website, www.privacy.gov.sk.ca, should be modified to address compliance with all parts of the *Freedom of Information and Protection of Privacy Act* and not just the Framework.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

4. Choices and Priorities

The *Health Information Protection Act* came into force September 1, 2003. By operation of section 1 (t) of *HIPA*, every government institution under the *FOIP Act* is also a "trustee" for purposes of *HIPA*. Each of those institutions has an important and significant responsibility under *HIPA* to do certain things.

> 16. Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:
>
> i. threat or hazard to the security or integrity of the information
>
> ii. loss of information; or
>
> iii. unauthorized access to or use, disclosure or modification of the information; and
>
> (c) otherwise ensure compliance with this Act by its employees

Most government institutions have significant volumes of personal health information for employees and in some cases citizens of Saskatchewan. The responsibilities of a trustee under *HIPA* are similar but different than the responsibilities of a government institution under the *FOIP Act*. We have encountered no government institutions yet that fully comply with the section 16 requirement. We note that although *HIPA* came into force more than 9 months ago, there are as yet, no regulations. The absence of regulations complicates compliance with *HIPA* but does not obviate the need to comply.

Although much work has yet to be done by government institutions to meet the statutory requirements of *HIPA*, we have found that many of those same institutions are committing resources to attempt to meet the requirements of the Framework. We find this disparity troubling.

Recommendation No. 7 -- All government institutions should ensure that compliance with section 16 of the *Health Information Protection Act* is given the priority the law requires and must take precedence over any Privacy Framework activities.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

5. Proposal for a Chief Privacy Officer

Appendix B to the Privacy Framework sets out a job description for a Chief Privacy Officer.

This appears to be an attempt to replicate what private sector organizations are doing under the *Personal Information Protection and Electronic Documents Act* without understanding key differences between public sector privacy regulation and private sector privacy regulation.

At first glance, the proposal for a Chief Privacy Officer ("CPO") seems to be a positive move. It suggests consolidation and centralization of responsibilities. A careful review of the job description however indicates that the CPO will contribute to fragmentation rather than integration of access and privacy requirements.

The job description makes no reference to compliance with the *FOIP Act* generally or to access to information requirements in particular. This appears to signal that the Saskatchewan government intends to subordinate access to privacy notwithstanding the contrary direction from the Saskatchewan Court of Appeal.

There is no discussion in the Framework of how the CPO will interact with the Chief Information Officer for Saskatchewan. Our concern is that creating a CPO may amount to balkanizing privacy work. It could operate in such a way as to relieve other key offices from taking appropriate responsibility for access and privacy work. We think it preferable to ensure that the job description of the Chief Information Officer for Saskatchewan includes responsibility to ensure compliance with the access and privacy requirements of the *FOIP Act* in all of the work undertaken by that office. This would likely be both more effective and more efficient for information in electronic format.

The one area in government that would clearly benefit from centralization is training for all government employees. This however would ideally be coordinated, not through a new stand-alone CPO, but through the Department responsible for administration of the *FOIP Act*. This is the subject of our Recommendations 1 through 6.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

5. Proposal for a Chief Privacy Officer (continued)

The *FOIP Act* in this province and every other province and territory has been deliberately designed to assign responsibility to each government department and individual Ministers. We think this is an important feature and ensures much clearer lines of accountability. Before the Framework, if an egregious violation of the Act occurred, responsibility would be that of the Minister responsible for that Department. Initially, the Office of the Information and Privacy Commissioner, and ultimately the Saskatchewan public must be able to hold that Minister fully accountable. If there is a Chief Privacy Officer "monitoring government operations", will this cloud or confuse the clear responsibility that the relevant Minister should have? Government is such a large entity that responsibility not clearly assigned to a specific Minister may diffuse the focus of accountability requirements. Our concerns might be allayed if other provinces had successful experience with a Chief Privacy Officer but we are unaware of such experience in the public sector outside of Saskatchewan.

We understand that the Ontario Information and Privacy Commissioner in her 2001 Annual Report had recommended the creation of a Chief Privacy Officer position for that province.[54] We note however that Ontario also has a very well-established access to information regime and presents a different set of needs than is the case in Saskatchewan.

It is not clear to our office that the creation of this new CPO position and the significant new resources that would entail would add any value to good privacy compliance by the Saskatchewan government. There are other, and in our view, more appropriate ways to achieve those things particularized in the job description that appears as Appendix B to the Framework.

Recommendation No. 8 -- The Chief Information Officer should be given specific responsibility for incorporating privacy protection in all information systems of the government and for ensuring that legislative requirements are met.

[54] Page 7, available at www.ipc.on.ca

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

6. Proposal for a 'Privacy Officer'

Appendix C to the Privacy Framework sets out a job description for a Privacy Officer.

The Saskatchewan Government currently has no uniform job description or even job designation for those persons variously described as Access Officers, FOI Officers or Coordinators, Access and Privacy Officers or Coordinators. In many government institutions this is a relatively junior position and refers to the person who physically receives and processes access to information requests. The decisions on what, if any, exemptions will be invoked is made by one of perhaps several different more senior persons in that institution. In many government institutions, the designated officer does not report to the Deputy Minister and would not routinely be consulted on a range of access and privacy issues including new programs that would impact either access or privacy. In some institutions, one person has been designated as the Privacy Office for purposes of the Framework and someone else, and often a more junior employee, is designated as the Access Officer.

In most other provinces, the FOIP Coordinator is a more senior official who delegates to others aspects of processing breach of privacy complaints and access to information requests. It is the Coordinator who will make the specific recommendation to the Deputy Minister as to what records or information should be disclosed. Again, in most other provinces, the FOIP Coordinator spends as much or more time providing advice internally to the Department on the design of new programs, forms and systems to ensure compliance with the FOIP Act as that person does actually processing complaints and requests. The Ontario Information and Privacy Commissioner has produced an excellent document, *Basic Took Kit for New Co-ordinators.* [55]

In every other province, FOIP Coordinators discharge this kind of function and do so in a way that integrates access to information and privacy responsibilities. Why have one person in the Department with responsibility for privacy and someone different responsible for access to information? The two are closely linked and indeed are both subject to a single statute overseen by a single Commissioner. Does the Framework recommendation not make communication between the OIPC and the Department more fragmented and less satisfactory? How do you ensure that messaging from the Privacy Officer is consistent and complementary to the messaging from the Access to Information officer? What additional cost is involved with this duplication of responsibility? Both privacy and access compliance requires staff training, preparation of materials and liaison with the OIPC.

The problem is compounded by the requirement that the Privacy Officer report directly to the Deputy Minister. This does not appear to be the current situation with the Access to Information Officer in those departments.

[55] Available at www.ipc.on.ca

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

6. Proposal for a 'Privacy Officer' (continued)

Recommendation No. 9 – For every government institution, there should be one person designated as the Freedom of Information and Privacy Coordinator with responsibility for the FOIP Act including both access and privacy requirements. This FOIP Coordinator should be a senior manager in the government institution and should report to the Deputy Minister.

Recommendation No. 10 -- The FOIP Coordinator should be required to do the following:

- **respond professionally and efficiently to access requests and privacy complaints;**
- **raise awareness of access and privacy issues on a regular and proactive basis within their organization;**
- **be well aware of all operations of the organization, the kinds of records and record-management systems in the department;**
- **be able to quickly identify what units within the department are likely to have the records responsive to an access request and which employees should be consulted;**
- **be senior enough to be able to provide access and privacy advice to the Deputy Minister or head of your organization on a regular basis;**
- **monitor decisions and recommendations of the OIPC and ensure those decisions are integrated into the orientation and in-service training of staff in the Department;**
- **be involved in the design of new programs that may impact access or privacy rights;**
- **provide timely advice to the Department to ensure that the FOIP Act will be complied with; and**
- **improve general awareness about the legislation and also substantive items such a specific recommendations from the OIPC. This can be done through regular in-service training sessions within a department. The Coordinator may undertake internal audits to identify areas where more work is required to ensure full compliance.**

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

7. Amending the *FOIP Act*

There is a need for review and revision of the *FOIP Act*. Although Part IV of the Act sets out a complete code for collection, use, disclosure, access to and correction of personal information, it should be strengthened. This can best happen not through the development of collateral instruments that have no legislative sanction but rather through amendment of the Act itself.

Mr. Richard Rendek, the former Acting Information and Privacy Commissioner, outlined a number of recommendations for statutory amendment in his Annual Report for 2002-2003. We agree with those recommendations. In addition, in our Annual Report for 2003-2004 we intend to enumerate a longer list of changes we propose to make the FOIP Act work better for government institutions and for the public.

Alberta has undertaken two reviews of its *Freedom of Information and Protection of Privacy Act* in 1998 and 2001. In each case this was done by a Select Special Committee of the Legislative Assembly. In each case the result was a number of amendments to that province's legislation to update and improve its usefulness. Similar reviews have been undertaken in British Columbia and Nova Scotia. Manitoba is currently reviewing its access and privacy statute by means of a working committee. We note that the province of Prince Edward Island is planning to review its access to information and protection of privacy law only two years after it went into force.

Recommendation No. 11 – The *Freedom of Information and Protection of Privacy Act* should be reviewed by an all-party committee of the Assembly to determine what changes to the statute and government policies and practices is necessary to ensure an adequate level of access and privacy in Saskatchewan.

Access to information and protection of privacy represent fundamental values of Canadian citizenship. The importance of both goals is reinforced by the paramountcy provision in section 23 of the *FOIP Act*.

It is important that citizens be able to refer to the *FOIP Act* for a clear understanding of what rights of access and privacy mean. This would be consistent with the movement to 'plain language' legislation and the importance attached to transparency in government. An explicit purpose clause in the *FOIP Act* becomes an important way of making such a statute more accessible to citizens and easier to understand for government employees. Since the Saskatchewan *FOIP Act* was proclaimed, most recent access and privacy laws in other jurisdictions have incorporated a purpose clause. This kind of clause has proven helpful to Information and Privacy Commissioners and superior courts in the interpretation of those statutes.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

7. Amending the *FOIP Act* (continued)

The office of the Saskatchewan Information and Privacy Commissioner has indicated that in interpreting the *FOIP Act* it views the purpose of this Act to be the same as the purpose clause in the British Columbia *Freedom of Information and Protection of Privacy Act*. In our view, this is consistent with the past practices of this office and the direction of the Saskatchewan Court of Appeal and Court of Queen's Bench.

Recommendation No. 12 – The *Freedom of Information and Protection of Privacy Act* should include an explicit purpose clause. We propose the following text:

The purposes of this Act are to make government institutions more accountable to the public and to protect personal privacy by:

(f) giving the public a right of access to records,

(g) giving individuals a right of access to, and a right to request correction of, personal information about themselves,

(h) specifying limited exceptions to the rights of access,

(i) preventing the unauthorized collection, use or disclosure of personal information by government institutions, and

(j) providing for an independent review of decisions made under this Act.

Perhaps the most conspicuous privacy gap in the *FOIP Act* is the absence of any express requirement that government institutions keep personal information safe and secure.

Recommendation No. 13 -- The *Freedom of Information and Protection of Privacy Act* should be amended to include a requirement that the head of a government institution must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and destruction.

VII SPECIFIC AREAS OF CONCERN AND RECOMMENDATIONS (CONTINUED)

7. Amending the *FOIP Act* (continued)

Since the *FOIP Act* was proclaimed we have witnessed the expansion of 'shared services' that require collaboration among multiple organizations. A shared service is a service that requires the involvement of more than a single government department. A good example is the SCHOOLPLUS model developed in Saskatchewan. SCHOOLPLUS contemplates the sharing of personal information between different organizations to better support children at risk. Some of these organizations may be departments, local authorities or organizations subject to the federal Privacy Act. The *FOIP Act* however is based on information collected and used within the department. Sharing personal information outside of a department is a disclosure and will typically require consent unless one of the prescribed circumstances in section 29 can be invoked. Our office has received reports of difficulties about implementing SCHOOLPLUS attributable to a lack of clarity and agreement around the rules that will apply. We are not advocating eliminating all privacy checks and balances in a shared service context but we do submit that this issue requires attention and likely legislative amendment to address.

Recommendation No. 14 -- The *Freedom of Information and Protection of Privacy Act* should be amended to permit the use and disclosure of personal information, subject to appropriate safeguards, to enable 'shared services' such as the SCHOOLPLUS initiative.

In contrast with the substantial penalties provided in more recent privacy laws, the only penalty for breach of privacy is an offence by way of summary conviction with a maximum fine of $1,000.

Recommendation No. 15 -- The *Freedom of Information and Protection of Privacy Act* should be amended to signal the seriousness of privacy breaches by increasing the penalties to something more substantial such as a maximum fine of $50,000 for an individual and $100,000 for a corporation.

(THIS PAGE LEFT BLANK INTENTIONALLY)

VIII CONCLUSION

In our opinion, the Privacy Framework has been constructed on some questionable assumptions and an apparent lack of understanding of Saskatchewan's FOIP regime. Nonetheless, the ostensible purpose of the Framework - stronger privacy protection-is important and worthwhile. In addition, the publication of the Framework and early efforts to build awareness among provincial government employees and Crown Corporations has certainly succeeded in emphasizing the importance that the government assigns to the privacy of Saskatchewan residents. Excellent initiatives are underway through the office of the Provincial Archives and the Chief Information Officer to improve record retention and disposition systems and to utilize information technology to improve privacy protection.

Government now has an ideal opportunity to revisit the Framework and to consider other steps to better achieve enhanced privacy protection for the people of the province. Our view is that such a goal can best be met by undertaking a comprehensive review of the *FOIP Act* and its administration.

Our office looks forward to working with the Saskatchewan Government to ensure Saskatchewan residents will enjoy the full measure of the access and privacy rights they have been guaranteed by the *Freedom of Information and Protection of Privacy Act.*